U-42-3

14-3

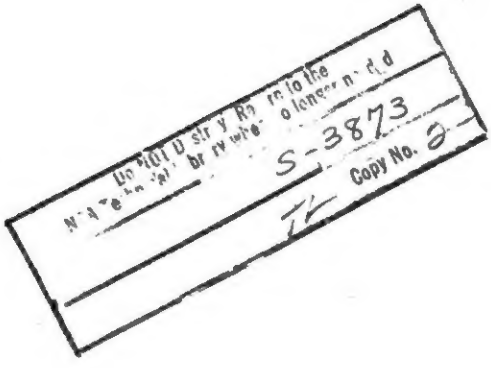
ARMY SECURITY AGENCY

117/49/TOPSEC/AS-14

Copy No. 6

CSGAS-14

To: AFSA 02A7



ORGANIZATION OF THE CRYPTOLOGIC AGENCY OF THE ARMED FORCES HIGH COMMAND, WITH NAMES, ACTIVITIES, AND NUMBER OF EMPLOYEES TOGETHER WITH A DESCRIPTION OF THE DEVICES USED

1. During his period of detention (September-December 1946) at the Hq 7707 European Command Intelligence Center, Oberursel, Germany Wilhelm FENNER, former Ministerialrat and chief of cryptanalysis in the Armed Forces High Command Cryptologic Agency (OKW/Chi), wrote a lengthy report concerning his past career and his extensive experiences in the field of cryptology. This report was never issued in translation although an inadequate summary by Army Security Agency was issued as TICOM/I-206.

It is presently planned to issue a complete translation of the entire report in the DF series (DF-187). The attached translation is the second of the series and is FENNER's description of the organization of OKW/Chi during the period 1939-1945.

December 1949 35 copies; 28 pages

Translated: RWP

Distribution: Normal

TABLE OF CONTENTS

		Page
I.	In the Year 1944	1
A.	Organization	1
	General	1
	Special	3
B.	Activity	12
	Basic	12
	Interception of Telegrams	12
C.	The Intercept Service	14
D.	Main Group B	15
	Telegram Registry	15
	Assignment of Cryptanalysts	16
	Strict Objectivity in Translating	16
	Security	17
	Relations with Friendly Cryptologic Agencies	17
	Reporting	17
	The Essence of Cryptanalysis	18
	Mechanical Cryptanalytic Aids	18
	Roellchengeraet	18
	Electric Typewriter	19
	The Dig Difference Calculator (Differenzengeraet)	19
	The Bigram Device (Bigrammgeraet)	20
	Phase Searching Device (Phasensuchgera..)	20
	Hollerith Machines	20
	Own Cipher Machines	21
II.	In the Year 1939	21-28

ORGANIZATION[1] OF THE CRYPTOLOGIC AGENCY OF THE ARMED FORCES HIGH COMMAND, WITH NAMES, ACTIVITIES, AND NUMBER OF EMPLOYEES[2] TOGETHER WITH A DESCRIPTION OF THE DEVICES USED.

I. In the Year 1944

A. Organization

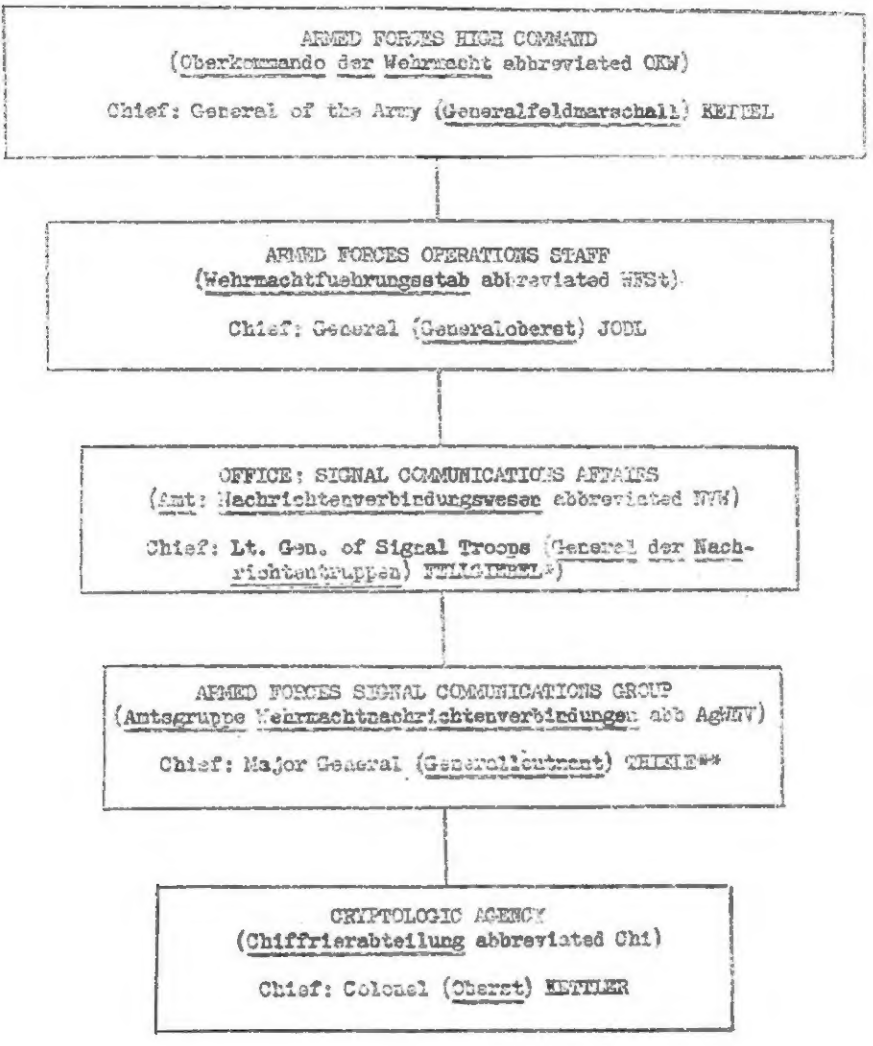
General: The Armed Forces High Command (Oberkommando der Wehrmacht hereafter referred to as OKW) was made up of offices with the most varied designations of which only a very few are familiar to me. One of these offices was the Armed Forces Operations Staff (Wehrmachtfuehrungsstab hereafter referred to as WFSt). Its vertical organization in regard to the Cryptologic Agency (Chiffrierabteilung hereafter referred to as Chi) may be represented as follows (See diagram on following page).

In peacetime Chi was an office of the Inspectorate of Signal Troops (Inspektion der Nachrichtentruppen hereafter referred to as In 7), out of which Signal Communications Affairs (Nachrichtenverbindungswesen hereafter referred to as NVW) had arisen by progressive organizational changes.

---

1. In view of the fact that more than a year and a half have passed since the dissolution of the Cipher Agency and that I have maintained no contact with the former members of this organization and possess no documents of any sort, many names have slipped my mind. Likewise details have escaped my memory. This account, however, agrees essentially with the facts.

2. An "employee" male or female, (Angestellter or Angestellte) is a person obligated by a civil service contract. Such a person is not engaged for life and has no claim to a pension. Such a person is not a member of the Armed Forces. An "official" of the Armed Forces (Wehrmachtbeamter) is not an officer and therefore never has disciplinary powers. He is appointed for his lifetime and has a claim to a pension. In contrast to civilian employees he is subject to military law (wears a uniform in wartime) but is allowed to choose his political party. A "detailed official" (beorderter Beamter) is an official of a non-military agency released for service with the Armed Forces. Although in Question A information was asked only regarding employees (Angestellten) i. e., civilians, I have also given the names of officers and officials insofar as I have kept the names in mind. I assume that in the word Angestellten these were likewise to be included.



*Later Major General (Generalleutnant) FRAUN. Both FELLGIEBEL and FRAUN were hanged after the attempt on HITLER's life 20.7.44.

**Later Major General (Generalleutnant) GIMMLER. Both THIELE and GIMMLER were hanged after the attempt on HITLER's life 20.7.44.

Special: Chi was composed of main groups, groups, and sections of which the abbreviations were:

Main Group (Hauptgruppe abbreviated H Gr)

Group (Gruppe abbreviated Gr)

Section (Referat abbreviated Ref)

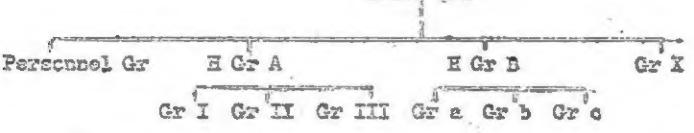
Directors or Heads of Sections were designated Leiter (abbreviated L). Thus, for example, LHGrB means Director of Main Group B (Leiter der Hauptgruppe B).

DIAGRAM SHOWING ORGANIZATION OF CHI

Chief Chi

Personnel Gr — H Gr A — H Gr B — Gr X

Gr I — Gr II — Gr III — Gr a — Gr b — Gr c



OUTLINE OF ORGANIZATIONS OF CHI WITH DUTIES AND PERSONNEL

Chi

Assignments: Own systems. Foreign systems. Obtaining intelligence by technical means.

Chief : Oberst[3] (Colonel) KETTLER

Deputy : Major[4] METTIG

Anteroom : Frl[5] Hedwig KUHNERT
Registry Frl _____ (position not always filled)
(TOP SECRET Documents)

Personnel Group

Assignments: Personnel, quarters, secret and open registry.

Director : Major d. R.[6] Dr. ....ER (?)

Anteroom : Frl MALLECK
Frl _____

Registry : Frl Anni BARTHEL
(Unclassified Frl _____
SECRET Frl _____
Documents) Frl
Amtsgehilfe 'LANGE
One or two male messengers

---

3. German titles (or their abbreviations) have been retained in the charts with approximate English equivalents given in the footnotes, thus Oberst (Colonel). [Editor's note].

4. [illegible]

Main Group A [8]

Assignment: Own cryptographic systems. Interception of foreign radiograms and cablegrams.

Director : Major METTIG

Anteroom : Frl VERNORN

Group I Director: _____

Assignment: Development, production, and distribution of own systems for Army, Navy, Air, agents in connection with the three branches of the Armed Forces. Checking own cryptographic systems with regard to security.

Personnel : Sdf.[9] Dr. FRICK

Reg. Oberinsp.[10] Fritz MENZER

Some 10 detailed soldiers and numerous printers including

Reg. Insp.[11] Alfred FUCHS.

Liaison official of the Navy, ORR[12] FRANKE

Group II Director: Hptm[13] GROTZ

Deputy : Amtmann[14] KLINGER

Assignment: Drawing up plans for monitoring foreign international radio traffic, interception of telegrams of foreign governments. Call names, waves, time schedules. Allocation of assignments to the intercept stations of Chi. Training of "intercept operators". Some 10 soldiers detailed in Group II.

Group III Director: Oberstlt.[15] KAEHLER

Deputy : Reg. Baurat Dip. Ing.[16] SALZBRUNN

---

8. I no longer recall the organization of this group.
9. Sonderfuehrer (Specialist Leader)
10. Regierungsoberinspektor (Government Chief Inspector)
11. Regierungsinspektor (Government Inspector)
12. Oberregierungsrat (Chief Government Councillor)
13. Hauptmann (Captain).
14. Official.
15. Oberstleutnant (Lieutenant Colonel).
16. Government Architect, Graduate Engineer.

Assignment: Monitoring and interception of foreign press and propaganda transmissions. Evaluation, translation, reproduction, and distribution of the most important items. Improvement of radio receiving stations. Telegrams from and to Chi. Uninterrupted 24-hour service.

Personnel : Some 100 civilians, male and female, whose names I do not know.

Main Group B

Director : Min. Rat[17] Wilhelm FENNER

Deputy : Min. Rat Viktor WENDLAND

Assignment: Decipherment (cryptanalysis) of cryptograms of foreign governments. Development of mechanical cryptanalytic aids. Training and instruction.

Liaison : FR SCHULZ (Air Force) analyst with Main Group B

Group a

Director : Oberlt[18] Otto KUNZE[19]

Anteroom (LHGrB) : Frl Hertha LIEBENBERG
Frl Anneliese NATHO
Frl Ilse FLOCKE
Frl Linda SCHOTT
One detailed soldier

Secretariat: Reproduction of deciphered messages. Log of TOP SECRET documents. Personnel, quarters, courier service.

Registry of Telegrams: Freifrau[20] Edith v. MEDEM
Frl Ilse SCHWAB
Frl KRENZ
Occasionally one or two detailed soldiers

Distribution of incoming encrypted telegrams to the several sections

---

17. Ministerialrat (Ministerial Government Councillor).

18. Oberleutnant (First Lieutenant).

19. Detailed for service with Chief of Chi. Group a was therefore personally directed by the LHGrB /FENNER/.

20. [illegible]ess.

Group b

Assignment: Practical (current) decipherment of cryptograms of foreign governments.

Director : Min. Rat Dr. Viktor WENDLAND

Deputy : Min. Rat Dr. Joseph Leo SEIFERT

Section b_1 -- (For Special Assignments)

Assignment : Preliminary studies of entirely new types of foreign cryptograms. Consultation on cryptologic matters.

Head : Professor Peter NOVOPASCHENNY

Statistical Clerks: Frl Erna ESLUHN
Angst.[21] Leonhard LERCH
In case of need also one female employee and two detailed soldiers

Section b_2 -- Yugoslavia

Head : Min. Rat Dr. Viktor WENDLAND

Members : Angst. Georg CRULL

Gef.[22] LOETS

Freiin von THIELMANN

Section b_3 -- Roumania

Head : Major Dr. Erich LENSCHAU

Members : Angst. Werner (?) DRAEGER

Angst. _____

Frl SCHRADER, typist

Section b_4 -- Italy

Head : OKR Franz-Karl RAFFEL

Members : Angst. Dr. Eugen MAULER

Angst. Werner TESSMAR

Funker[23] Corvin SCHNELLBACH

Angst. _____

Frau HAUSMANN, Frl PETZOLD, Frau Charlotte FUCHS.

Two female typists

2[1] -estellter (Employee).

Section b_5 -- France, Belgium, Netherlands, Switzerland, Egypt

Head : ORR Dr. Helmut MUELLER

Members: Angst. Studiendirektor a. D.[24] (Employee, PEDERSEN)

Oberlt. d. R. KUNZE, Otto [25]

Frau Elise KUNZE

Frl von KUNOW

Frl Mathilde TENNER

Angst. Dr. ____

Angst. Rudolf TRAPPE

Frau ____ (SCHROEDER ?)

Frl ____

Two female typists and eight assistants

Section b_6 -- England, USA

Head : ORR Nikolai ROHEN

Members: RR Dr. DENCKER

RR Dr. Franz WEISSER

RR Helmut SCHULZ

Angst. Robert MORS

One detailed official KALLE, Frl Irmgard (?) HELLER, Frl Irmgard KOEPP, Frau Anne BEHNINGHOVEN, Angst. Siegfried POST, Frl Dr. Margarethe BRUSSOW, and some 12 additional male and female employees as statistical clerks and typists.

Section b_7 -- Sweden, Norway, Denmark

Head : RR Theodor WEVERINCK

Members: Uffz.[26] SCHWEDE

Frl SCHWEDE

Frl Gerda (?) FUNK (?), typist

Soldat[27] MUELLER

---

24. Master (Retired).

Section b_8 -- Spain, Portugal, Latin America

Head : RR Karl KIEFER

Members: Two or three Uffz.

Angst. HODERLEIN

One female employee as typist

Section b_9[28] -- Agent systems

Head : Oberlt d. Res. Dr. _____[29]

Members: Some 10 sergeants and enlisted men

Section b_{10} -- Turkey

Head : RR Dr. Habil. Ernst LOCKER

Members: Angst. Alfred WITTE

Angst. KLEIN

Uffz. Martin GEMPERLE

Frau FUCHS, typist

Frl KLEIN, typist

Three detailed soldiers

Section b_{11} -- Greece

Head : Min. Rat J. L. SEIFERT

Member : Frl Gertrud BAULE

Section b_{12} -- Vatican

(Occasionally worked on by Min. Rat J. L. SEIFERT)

---

28. Possibly this section had a different number.

29. Not taken over by the Army until late in 1944.

Section b_{13}	--	Japan, China
Head :		Oberlt d. Res. Dr. ADLER
Members:		Three Uffz.
		Frl MALLE, typist
Section b_{14}	--	Iran
Head :		RR Dr. Ernst LOCKER
Member :		Uffz. Dr. HANSEN
Section b_{15}	--	Not staffed
Section b_{16}	--	Poland
Head :		beorderter Beamter[30] Edgar BERNDT
Members:		Frl Elisabeth WALTER
		Uffz. BRASCHE
		Some 13 detailed sergeants and enlisted men
Sections b_{17-21}	--	Not staffed
Section b_{22}	--	Bulgaria
Head :		OKR Ernst ROTTER
Members:		Soldat Dr. LUETJEN
Special Section	--	Military dictionaries
Head :		Sdf. KUEHN
Members:		Three enlisted men
		One female typist

30. **Detailed official.**

Group c

Assignment: Analytical solution or reenciphernents. Testing of cryptographic inventions. Development of cryptanalytic aids. Training and instruction.

Director : RR Dr. Erich HUETTENHAIN

Deputy : Cryptanalysis: Prof. Dr. FRANZ, University of Giessen

Technology : Reg. Beurat Dip. Ing. Wilhelm ROTSCHEIDT

Anteroom : Frl KRAUSCH

Section c_1 -- Analytical solution of foreign reenciphernents

Head : Professor Dr. FRANZ

Members: Geh. Professor Dr. ____, University of Hamburg (theoretical expert of the group)

beamteter Beamter Prof. Dr. WEBER, University of Berlin

beamteter Beamter Prof. Dr. SCHULZE (?) University of Erlangen (?)

Some 60 male and female employees and detailed enlisted men as statistical clerks and typists

Section c_2 -- Testing of cryptographic inventions

Head : Lt[31] d. Res. Dr. STEIN

Member : Oberlt d. Res. HASENJAEGER

Section c_3 -- Development of cryptanalytic aids

Head : Reg. Beurat Dip. Ing. Wilhelm ROTSCHEIDT

Members: Some 10 detailed enlisted men as able machinists and draftsmen

---

31. Leutnant (Second Lieutenant).

Section c_4 -- Training and instruction of new cryptanalytic generation

Head : IR Dr. HUETTENHAIN with Min. Rat FENNER and Min Rat Dr. WEYELAND as instructors

Main Group X

Director : Oberstlt Willibald von KALCKSTEIN

Deputy : Major d. Res. Dr. SCHAFFNER

Anteroom : Frl ____

Assignment: Scanning and forwarding of deciphered foreign telegrams to the competent offices. Day book with the contents of the most important telegrams. Secret information card file.

Section X -- Scanning and forwarding of deciphered telegrams. Day book.

Head x : Oberstlt Willibald von KALCKSTEIN

Members : Major d. Res. SCHAFFNER

Section Y -- Carding items from deciphered messages and from plain-text messages of the international press. Carding by family and place names, subjects such as politics, economics, military matters. Distribution of secret information.

Head : Wm.[32] Dr. Herbert SCHAEDEL, Instructor University of Leipzig

Members: Uffz. ARIUS

Three female employees and one enlisted man as assistants

---

32 Wachtmeister (Sergeant).

B. Activity

Basis: The uppermost principle in Chi as an agency procuring intelligence was speed. Therefore this principle always prevailed in the assignment of the work and the distribution of personnel. Any old organization is apt to become an end in itself as soon as its organism becomes weak and the morale of each member becomes questionable. Any such danger existed for Chi only in those groups which had no contact with friendly, similar organizations. Where such a contact did exist, however, there was regularly a wholesome competition. Such friendly organizations included:

a. The Cryptologic Agency (Chiffrierabteilung) of the Royal Hungarian General Staff in Budapest,

b. The Cryptologic Agency of the Finnish General Staff,

c. The Cryptologic Agency of the Royal Italian General Staff in Rome,

d. The Cryptologic Agency of the Foreign Office (Auswaertige A... in Berlin,

but not:

e. The "Research Bureau" (Forschungsamt) of Hermann GOERING which had been founded in 1933 without any national necessity as a purely personal enterprise of the then Prussian Prime Minister.

Interception of Telegrams: The primary factor in any information obtained by technical means was:

a. The radiogram,[33]

b. The cablegram,[34]

c. The overheard telephone conversation or plain correspondence,[35]

d. The radio-telephone.[36]

---

33. In order to be as independent as possible in the matter of foreign enciphered messages, Chi had two Armed Forces receiving stations (Wehrmachtfunkempfangsstellen): in Treuenbrietzen and in Lauf. The director of such a receiving station was always an officer of the signal troops, who was assisted by a technical official of medium grade (von einem technischen mittleren Beamten). Main Group A of Chi issued orders as to which foreign transmitters were to be covered. The director of the receiver station set up the local operational plan. He was responsible for the exact training of radio operators as so-called "intercept operators". I am not informed about the personnel strength of an Armed Forces receiving station. The intercepted enciphered messages were, almost without exception, sent in three copies by mail or by courier to Main Group B of Chi. For Chi had undertaken to pass one copy of each cipher radiogram to the Foreign Office and one copy of many cipher radiograms to Budapest. Whatever was important according to the instructions of Main Group B was forwarded from the receiving station in conjunction with Group B immediately to Chi by Siemens high-speed teleprinter.

If Group III had any time to copy foreign cipher messages of certain transmitters in addition to foreign press and propaganda transmissions, then this was done. For the short route from one office of Chi to another office of Chi without going through a central telegraph office and various offices of registry was important, particularly in critical periods. But the Cipher Sections in Finland, Budapest, and Rome also sent duplicates of their radio intercepts by courier; Budapest in urgent cases by telegraph. Finally even the Forschungsamt made available a duplicate of its radio intercepts.

34. After the founding of the Forschungsamt in the spring of 1933 it claimed, ostensibly on the basis of a so-called "Order of the Fuehrer", the sole right to receive from the main telegraph office in Berlin and from provincial telegraph offices copies of cablegrams. From that time on, the Forschungsamt as intermediary provided the Cipher Sections with duplicate cablegrams which prolonged unnecessarily the time between the moment of sending and the decipherment of each message, and regularly occasioned friction between the services. Budapest, Helsingfors, and Rome also turned over to Chi duplicates of enciphered cablegrams obtained there. Budapest sent all its material once a week; Helsingfors about twice a month; Rome quite irregularly. At irregular intervals Main Group B also received duplicates of cablegrams and radiograms from Madrid and Sofia without knowing who sent them.

35. This was the domain of the Forschungsamt. Just as in the case of censorship of letters, Chi had nothing to do with this aspect, with the limitation that occasionally letters with secret text were referred to Main Group B to be worked on.

36. Was worked on in Main Group A III insofar as press and propaganda were concerned.

Hence, traffic receipts at Chi came from

a. The Germ Armed Forces radio receiving stations

b. Budapest

c. Helsingfors

d. Rome

e. Main Group A III

f. Forschungsamt

g. Madrid and Sofia

Using these sources, it was possible to pick up with a high degree of probability all important encrypted telegrams even in case of atmospheric disturbances and when telegraph lines by-passed Germany. Of course, courier pouches were safe against such interception.

C. The Intercept Service

I have only a superficial acquaintance with the specific activity of Main Group A. From my point of view it is of interest only as a means to an end. From the standpoint of cryptanalysis it made no difference what organizations furnished the encrypted messages; the cryptanalytic section needs the messages and makes this need known. The competent agencies have to fulfill this request as far as possible. It is self-evident that the Berne List is not adequate for the organization of a complete intercept service: constant changes and frequent deviations from the rule make it necessary that experienced people work over the assignment of the intercept range, take into account local disturbances, and in particular solve the problem of intercepting with a limited number of intercept operators from the gigantic mass of international radio traffic only those messages which are really important. Radio operators suitable for the intercept service always needed when they came from the Army a period of special training before they could work independently without constant supervision. The length of this training depended primarily on the "acoustic" talent of the intercept operator, i. e., on the selectivity of his ear and on h' eaction speed. Only secondarily did routine instruction regarding form a tent of telegr[illegible] calligraphy, and the making of several copies

come into account. In view of the necessity of being sparing of personnel, technical aids were used in the intercept service and these were indispensable for high-speed telegraphy. I am not acquainted with these devices I do know however, that among other things magnetophones were used - demagnetized steel wire susceptible to magnetization. The number of instruments in use, the models, and manufacturers are not known to me. It goes without saying, however that the development of foreign transmitting mechanisms naturally found a parallel in the development of receiving mechanisms. Group III achieved good results with blind intercept operators; the exactness and correctness of their work was highly esteemed.

D. Main Group B

Telegram Registry: An organically important office of Main Group B was the Telegram Registry. Here hundreds of messages, sometimes far over a thousand, passed through daily. This material had to be worked over immediately and for that reason the personnel began work earlier than the cryptanalysts who had to find the sorted traffic ready for them when they started work. During the work of registration the duplicates for the Foreign Office, Budapest, Helsingfors and the Forschungsamt were separated out at once, likewise telegrams of countries not worked on and such discards as congratulatory telegrams in plain text. Statistical work in the Registry was limited to counting the in-coming telegrams according to the individual countries and was broken down into radiograms, cablegrams, and discarded messages. More complicated statistical studies were intentionally omitted in order to eliminate all unnecessary office operations. However, if Group I of Main Group A needed for any reasons whatsoever an exact survey of the traffic, e. g., by wave lengths, call signs, and times, the material was available to its expert during the sorting, or he himself could go to the cryptanalysts and look at the messages. The daily log sheets kept at the intercept stations all came to Group I anyway so that as a rule the necessary check was made without burdening the Telegram Registry and the cryptanalysts. If, when sorting the messages, anything turned up which ran counter to the rule, this was immediately reported to Group I. All unnecessary

paper work, however, was avoided. What could be settled by telephone was cared for in that way; otherwise, a slip of paper was enough. Group I likewise passed on anything it considered important so that there was always intimate contact among the Telegram Registry, cryptanalysis, and intercept.

Assignment of Cryptanalysts: In actual cryptanalysis the procedure was in accordance with the following natural principle: the experienced cryptanalysts worked on new codes and solved all reencipherments, insofar as the task did not exceed their abilities or the potential of the section concerned; the less experienced and less well trained cryptanalysts were occupied with the current expansion of codes already solved to a fair degree, while the beginners decoded telegrams in systems already solved. In each language section there were also typists and several statistical clerks to perform auxiliary tasks as needed. As a rule, these were persons who did not know the language or had only an insufficient acquaintance with it. On the other hand, first class philological mastery of the foreign language was expected of every cryptanalyst; the nuances of the official language were learned by practical work.

Strict Objectivity in Translating: As soon as the encrypted telegrams had been decoded, i. e., the code groups had been transformed into plain text, they were immediately translated into German. An experienced analyst dictated the German text directly to the machine. The translation was literal but in excellent, standard German (Hochdeutsch); only in very rare cases was the original word added in parenthesis when there was doubt or when there was no correct equivalent in German. It was strictly forbidden to make summaries. Likewise the decipherer had to refrain from any subjective remarks. And it was his duty to put a dotted line under any word or passage in the German text which was not absolutely sure, thus honestly confessing to those working over the text in other agencies where there might be something inexact in the German text, so as not to lead to false conclusions. Likewise when there were gaps in the messages the decipherer had to state in the German text how many groups were missing. There was an agreement with Chi that any questions raised there should be [illegible]d at once to the cryptanalytic section so as to give the latter a chance

Security: All traffic, the materials used in dealing with it, the results of decipherment and the methods employed were considered "TOP SECRET" ("geheime Kommandosache"). Every person was obligated to maintain secrecy. Every three months special instructions were given on this point. The doors of the rooms were unlocked only during working hours and then only if someone was in the room; otherwise, the doors were always locked. Moreover, all cryptographic material was kept in metal safes. The holder of the key was personally responsible for safeguarding the material according to regulations. He was checked four times a year to see whether he actually had the keys to all the safes. The loss of a safe key or the loss of operational material had to be reported within 24 hours at the latest. As a matter of principle female personnal were not allowed to have keys to safes. After the close of work, everything had to be put away and locked up; nothing was permitted to remain lying on tables. Daily room checks assured compliance with this order.

Relations with Friendly Cryptologic Agencies: The relations of Main Group B with the cryptologic agencies of friendly countries imposed on the sections, along with their current work, the obligation of seeing to it that the material called for was made available. That meant copies of telegrams, recovered code groups, and solved reencipherments. This material was delivered by the individual language sections to the anteroom of Main Group B, was provided with a brief letter of transmittal, and was sent to the recipient. The relations with Chi inaugurated by Budapest in the fall of 1922 were interrupted by military events early in 1945; Chi had established contact with Helsingfors in the spring of 1927; these lasted until the capitulation of Finland; in the spring of 1938 Rome entered into an agreement with Chi. These relations were broken off by Chi a few weeks before the Allied landing in Sicily.

Reporting: Down to the "Assumption of Power" (January 1933) an extensive report on the practical results of decipherment was written every three months, but with 1933 that stopped short. The reason lay in the mistrust of the For[illegible]hungsamt, which had meanwhile been founded and which, it was suspected, mi[illegible]y to take over the issue of the quarterly reports on the basis of an

"Order by the Fuehrer" in order to emphasize its own accomplishments. Therefore from 1933 on only annual reports were written and these were without any details whatsoever.

The Essence of Cryptanalysis: Cryptanalysis was regarded as a discipline closely associated with the theory of probability, in which the elements of the probability are of a linguistic nature. The work was carried on according to methods which are probably the same in the cryptanalytic organizations of all civilized countries. At the same time everything was avoided which might have turned this secret service into a mysterious one: pretentious virtuosity and "Black Art" were not recognized. Due to the dearth of personnel, mechanical cryptanalytic aids were used to gain time and to avoid errors, but only when their employment was regularly and permanently necessary. This means that when little traffic was received, all cryptanalytic work was done by hand. The basic idea of every mechanical cryptanalytic aid was to replace the speed of fingers in statistical operations.

Mechanical Cryptanalytic Aids: These were devices to aid in cryptanalysis.

Zeilschengemat.[37] A device consisting of 10x10 cylinders with the

---

37. Of the description of the Rollmaschine which was in use at the German Navy signal intelligence agency (OKM 4 SKL/III) as given by Lt. MORGENROTH of OKM 4 SKL/III (TICOM/I-117):

> "Rollmaschine. The expression rollen for the production of "synthetics" arose from the use of a small apparatus to assist in the process, called a Rollmaschine. This consisted of 4 or 5 drums (glass tubes gummed over with paper strips), on which the figures 0-9 were printed, one underneath the other, running around the tube. This was arranged in such a fashion that when the Rollmaschine was set at the "neutral" position (0000) the figures expressed the values of known book groups. We also had Rollmaschinen which instead of the glass tubes had movable type wheels on metal rods, so that by changing the position of the wheels we could carry out the process of rollen again and again with other frequent groups, which was not possible with the glass tubes, owing to the fixed arrangement of the figures. When we turned (rollte) the drums so that instead of the original setting 0000, the value of a message group appeared, then we had automatically added the message groups to all frequent book groups recorded by the machine and formed Verdachtswuermer (Message group plus book group equals subtractor group). If we have set up not true book groups but relative book groups on the machine, then we naturally obtain a relative Verdachtswurm."

[illegible] [illegible] [illegible] [

The Bigram Device (Bigrammgerat). This consisted of some 26^2 relays corresponding to the number of bigrams normally possible. In appearance it was an upright metal frame over 200 cm high and some 100 cm wide to accommodate the relays. For study by means of this device the messages had to be punched in the tapes. Then all hole sequences of tape I were automatically brought into coincidence to all hole sequences of tape II. The result was read off and, as I recall it, reproduced graphically on a paper tape. If, at a particular position of the two tapes, frequencies of expected natural bigrams resulted, then a so-called "weak point" of the cryptographic system had been found with a certain probability. In contrast to the differencing device (Differenzengerat), this device scanned in each position a series of hole sequences which had been empirically determined before setting up the machine. The device was occasionally used successfully in solving Japanese cryptograms but it was too sensitive for steady use. It was developed and constructed at Main Group B.

[illegible] device (Phasengerat). If it was expected that a frequently repeated plain [illegible] in a cipher message then this device served for the automatic detection of this phase. The cipher text was punched again and by scanning was registered via relays in the form of short graphic strokes on a paper tape about 30 cm wide. If this tape was now displaced by one whole sequence with relation to its initial position and scanned again (parallel to the first graphic recording) then with like sequences of holes there would be a closer sequence of symbols which could be detected by eye. Finally, if phase L_1 lay beside phase L_2 then on the basis of probability peaks would appear on the paper tapes which were visible to the eye and which were higher than at points where phases L_1, L_2 ... L_n did not lie side by side. A like interval between peaks was phase 1 assuming that $L_1 = L_2 = L_3 \ldots = L_n$. The device was never put into practical use. It was developed and constructed for experimental purposes at Main Group B.

Hollerith Machines: When great masses of Polish cipher messages had to be combed on, then they were sent to the "Machine Records" section with a

[illegible] consequently the future problem of mechanical aids to cryptanalysis pointed toward the creation of an optical scanning device because all mechanical devices worked too slowly

Own Cipher Machines. The development of our own cipher machines rested with the Ordnance Office (Waffenamt). Chi was supposedly involved in the criticism and analysis of the devices but Chi only made suggestions without constructing them itself. The Enigma was regarded as antiquated, although it was secure when properly used. The Geheimschreiber, the so-called 'G-Schreiber' was modern but not mobile enough. By the end of 1944 the developments planned were already doomed. No further practical work could be done.

II. In the Year 1939 (Shortly before the Outbreak of War)[38]

Chi

Assignment: Obtaining intelligence by technical means. Foreign cryptograms

Director : Oberstlt Fritz ROETZEL

Deputy : Major ANDRAE

Anteroom and Journal of TOP SECRET materials : Frl Hedwig KUHNERT

Chi consisted of four Groups:

Group I	Group II	Group III	Group IV
Major ANDRAE	Eptm ERENSKE	Major KAEHLER	Min. Rat WENNER
Employment of technical and personnel resources to obtain encrypted messages	Personnel General registry of the Cipher Bureau	Interception of foreign press and propaganda	Decipherment of foreign cryptograms

38. Chi passed from peace status to war status without change in organization. So far as I recall, plans had been drawn up about 1938 respecting probable personnel requirements in case of war. But the requirements then set forth were satisfied with approximately 30 percent increase in total personnel. More specific statements lacked any reasonable foundation because at that time no one knew who would wage war and therefore no critical points for expanded effort could be indicated.

Chi, which in 1939 was still known as Cryptologic Bureau (Chiffrierstelle), was, when the war broke out, a component part of the Inspectorate of Signal Troops (Inspektion der Nachrichtentruppen); hence Chi was not yet an "agency" (Abteilung). Its horizontal organi[illegible] appears above.

Each group consisted of sections, but I no longer recall the organization of Groups I, II, III.

Group Chi I

Director: Major AMIRAL

Deputy : Min. Amtmann[39] KLINGER

The range of assignments was, basically, no different from that in 1944 - but without the development and testing of German cryptographic systems. The Armed Forces receiving stations, Treuenbrietzen and Lauf, worked as so-called fixed radio receiving stations (Feste Funkempfangsstellen). Along with these there were fixed radio receiving stations of the Cipher Bureau in Koenigsberg, Breslau, Muenster, and perhaps two or three other places. The out-stations, Madrid and Sofia, had already been established, unless my memory deceives me. There were two receiving stations with slight personnel. If I am not mistaken, Madrid was commanded by Leutnant (Second Lieutenant) PLANKERT; Sofia by Oberleutnant (First Lieutenant) GROTZ.

Group Chi II

Director	:	Rotm (E)[40] BRUNSKE
Deputy	:	Uffz SCHULTZ
Secretary	:	Frl MOLLEK
Assignments:		As for Personnel Group 1944
Accounting	:	Two detailed sergeants
		One male employee
Registry (UNCLASSIFIED)	:	Frl BARTELL Frl Angst. LANGE Angst. SCHROETER, Alfons One male messenger

---

39. Ministerial Amtmann (Ministerial Official).

40. After 1934, a number of First World War officers were recalled, mostly in administrative positions, as supplementary officers (Ergaenzungsoffiziere) and designated as aktive Offiziere (E): the (E) was later dropped and those who were qualified were taken into the regular officer corps. [Editor's note].

Group Chi III (Technical Devices)

Director : Major KAMMER

Deputy : Reg. Baurat Dip. Ing. SALZBRUNN

Assignments: As for 1944

Personnel : The total strength in 1939 shortly before the outbreak of war may have been about 70 persons

Group Chi IV

Director : Min. Rat FEHNER

Deputy : Min. Rat Dr. SEIFERT

Intercom : Frl Martha LIEBENBERG

Assignments: As in 1944

Section IVa

Director : Min. Rat FEHNER

Assignments: As in 1944

Office : Frl LIEBENBERG

Frl MAIHO

Frl Irmgard KOEPP

Telegram Registry : Freifrau v. HEDEMANN
Frau SCHWAB
Frl ESLUEN
Two detailed enlisted men

The a-Section embraced the entire administration: telegram receipts, registration, personnel, quarters, correspondence, etc. On the other hand, all b-Sections were units for practical decipherment. [An outline of the b-Sections with personnel appears below.]

Section	Country	Personnel	Remarks
IVb	Russia Poland	Prof. Peter NOVOPASCHENNY Frl WALTER Frl FUCHS Angst. MERCH Angst. Dr. LUETJEN Angst. FLISCH, Alexander About 5 more persons	Working on Russian cryptographic systems and Polish Army and diplomatic ciphers.

Section	Country	Personnel	Remarks
IVb$_2$	Yugoslavia	OFR Dr. Viktor HERDLAND Angst. Georg CRULL Angst. LOKYS Angst. Freiin Ruth v. THIELMANN	
IVb$_3$	Romania	Hptm (E) Dr. Erich LEMSCHAU Angst. DRAEGER	
IVb$_4$	Italy	RR Franz-Karl RAFFEL Angst. TESSMAR Angst. MAURER Angst. Frau HAUSMANN Angst. Frau FUCHS Angst. Frl PETZOLD About two other persons	
IVb$_5$	France Belgium Netherlands Switzerland Egypt	RR Dr. Hellmuth MUELLER Angst. TRAPPE Angst. St. a. D. PEDERSEN Angst. Otto KUNZE Angst. Jakob CRULL Angst. Frl Dr. von KUNOW Angst. Frl FENNER Angst. Frau HUHN Angst. Dr. Angst. Dr. DUBOIS Frl Helene KOENIG About 6 other persons	Worked on Fred. " " "
IVb$_6$	England USA	RR ROHEN Angst. Dr. BERCKER Angst. Helmth SCHULZ Angst. Dr. WEISSER Angst. POST Angst. AMMANN Angst. Frau BEETHOVEN Angst. Frl Dr. Margot BRUESSOW Angst. Frl MUELLER Angst. Frl FLOCKE About 3 other persons	
IVb$_7$	Denmark Sweden Norway	Angst. Dr. Theodor WEVERINCK	
IVb$_8$	Spain Portugal Latin America	Angst. Karl KLINGER Angst. HODERLEIN	
IVb$_9$	Hungary		Systems worked only temporarily and with success. Expert: Min. Rat Dr. SEIFERT

Section	Country	Personnel	Remarks
IVb 10	Turkey	Angst. Dr. Ernst LOCKER Angst. Alfred WITTE Angst. Rudolf KLEIN Angst. Frl KLEIN	
IVb 11	Greece	Min. Rat Dr. [illegible] Angst. Dr. BRUCKMANN Angst. Frl Gertrud BAULE Angst. Dr. POSSINGNUS	
IVb 12	Vatican	Min. Rat Dr. [illegible]	
IVb 13	Bulgaria	RR ROTTER	
IVc	Analysis	Angst. Dr. Erich HUETTENHAIN Frl KRAUSCH Angst. GRAESSER (Herbert?) Angst. Dip. Ing. Wilhelm ROTSCHEIDT Tech Reg Insp[41] Fritz MENZER About 10 other persons	The c-Section is the crypt-analytic sectic
IVx	Distribution of decrypted messages	Oberstleutnant (E) von KALCKSTEIN Angst. Frl [illegible]	

A comparison of the organization of 1939 (shortly before the beginning of the war) with that of 1944 (shortly before the end of the war) shows that in the operational offices of the "Cryptologic Bureau OKW" and the "Cryptologic Agency OKW"[42] nothing essential has changed. The following difference, however, is important: whereas in 1939 Chi OKW worked on German Army cryptographic systems only in an advisory capacity and with voluntary checks or else merely developed German Army cryptographic systems, if the Inspectorate of Signal Troops (the Army

41. Technischer Regierungsinspektor (Technical Government Inspector).

42. When a section or a group through natural or unnatural development becomes so large that the director of such a unit must be a colonel, then this unit becomes an "Agency" (Abteilung). Every colonel who is transferred to OKW counted on becoming the "Chief of Agency" ("Abteilungschef".) The "Abteilungschef" corresponds to a regimental commander in the field. This is an old tradition, which under normal conditions was the expression of a necessary order (Ordnung).

requested it, in 1944 the entire development of German Army cryptographic systems had devolved upon the Cryptologic Agency (OKW). Aside from the personal wishes of the last Chief of Armed Forces Signal Communications (Chef Wehrmachtnachrichtenverbindungen abb. Chef WNV), Generalleutnant GIMMLER, the following purpose had been partially accomplished in the process: concentration within the Cryptologic Agency of all own cryptographic systems of all three branches of the Armed Forces, including those of the Protective Guard (Schutzstaffel abb. SS) and of semi-military organizations. (In the German Armed Forces each branch, i. e., Army, Navy, and Air developed the cryptographic systems it required without any testing or criticism by the other branches of the Armed Forces if it did not so desire!) This idea was good; its realization would have been desirable for obvious technical reasons, all the more so since I had already fought for it many years in vain. For, in spite of the point "OKW", the three branches of the Armed Forces were so independent that an order issued in 1943 (or perhaps early in 1944) for the common development of all Armed Forces cryptographic systems at Chi OKW was obeyed sometimes not at all, sometimes only reluctantly. But the mistake in the organization of Chi 1944 was that for personal reasons the development of cryptographic systems for the German Armed Forces was not assigned to Main Group B, but to a group which was broken off from it. Main Group B with its experienced cryptanalysts was active in an advisory capacity - whenever one desired to call upon it. This curious organization did not get to function!

Then it is noticeable when comparing Chi 1939 with Chi 1944 that the latter had considerably more personnel. That was a matter of course: Chi was an office which provided intelligence. During a war the exchange of information between the civilized peoples involved, and those not involved, is always greater than in peacetime. Therefore there are more telegrams. For a war affects the quantity of encrypted messages just as a chronic period of crisis would. Furthermore, press and radio propaganda appear in inconceivably increased measure. As a matter of course this results in a greatly increased [illegible] of personnel. At the same time really new experts were added in only

modest measure, as the comparison shows, while there were two or three times as many typists, translators, intercept operators, statistical clerks, draftsmen - in short auxiliary personnel.

In 1939 there were still no mechanical aids to cryptanalysis. All problems occurring up to that point had been worked on or solved without mechanical aids. Masses of telegrams had appeared until then only during brief periods of crisis (e. g., occupation of the Rhineland, the Chamberlain Line, occupation of Austria) and this material was worked up in a few day and night shifts. Consequently until 1939 there was no need of mechanical aids to cryptanalysis even though the fancy of some analysts had been occupied with this idea and experimentation had shown clearly that only the academically trained modern communications engineer would be equal to such a task.

Section IV b X still belonged to Group Chi IV: consequently the entire course of the work from the registering of the encrypted message to its solution and distribution was still in the hands of a single organism. The entire organization of the Cryptologic Bureau was clear and easily comprehended: I: the employment of the intercept organization for the interception of telegrams (secret text); II: the assignment of personnel; III: the technical communications group for intercepting press and propaganda (plain text); IV: the decipherment of foreign cryptograms. Until 1939 (outbreak of the war) Group IV was unquestionably the focal point of the Chiffrierstelle; in view of the mass of foreign press and radio reports (propaganda) which are easier to understand than the content of an encrypted message, which a layman does not understand, Group III gained in preponderance. (An objective study of this phenomenon, in particular comparisons with other countries might be very instructive.)

The relations with friendly cryptologic agencies were strengthened in 1939 with the exception of Rome. Regarding Rome there were arguments in OKW: part of the officers of OKW proper maintained that they knew nothing of any connection of the Cryptologic Bureau with the cryptologic agency of the General S[illegible] in Rome - and forbade any further connection; another part ordered

[illegible] and [illegible] under [illegible]. These relations were not broken off, not in account of HITLER's order but rather [illegible] and already [illegible] some things from Chi and a retreat now would have been foolish. Even between the cryptologic branch of the Foreign Office in Berlin and Chi OKW "peace" prevailed. Uncomfortable for Chi was the pressure of the Forschungsamt: it was always [illegible] about handing over encrypted cablegrams and radiograms, it was decrypting itself with a cryptanalytic staff which was supposed to be three times as great as Group Chi IV. There was a friendly exchange of traffic and of cryptanalytic results with the Foreign Office in Berlin, however, and so the Forschungsamt obtained from the Foreign Office and that Chi had solved since the Foreign Office got every key solved by Chi. Thus Chi OKW was engaged in a war against an as yet unknown number of "foreign foes" whose weapons were their cryptographic systems; the "inner foe", which caused far more vexation, was the Forschungsamt of Herrn [illegible] GOERING who had [illegible] become Reichsmarschall.

There is a special reason why a number of [illegible] employees (Angestellter) of Group IV 1939 are [illegible] in the table of Organization of Main Group 3 1944 as officials (Beamten). Chi as a cryptanalytic organization calling for special training also had a special career system. To the outside world it was known as the "Superior Foreign Language Service of the Armed Forces ("Hoeherer Fremdsprachendienst der Wehrmacht"). Cryptanalysts, who had the requisite preliminary education, could upon passing special courses at Chi take the second (grand) state examination and then - as vacancies arose - become Government Councillors (of the Superior Foreign Language Service of the Armed Forces - Cryptanalysis) in OKW.[43]

---

43. Regierungsraete (der hoeheren Fremdsprachendienstes der Wehrmacht - Entzifferung).